LIBYAN ACADEMY FOR TELECOM AND INFORMATICS

SECURITY + SY601 COURSE MODULE4

Instructor Khaled Gamo

Module4 Operation and Incident Response

Tools/Assess Organizational Security

This chapter covers CompTIA Security+ exam
objective 4.1: Given a scenario, use the appropriate tool to assess organizational security.

Network Reconnaissance and Discovery

tracert/traceroute

nslookup/dig

ipconfig/ifconfig

nmap

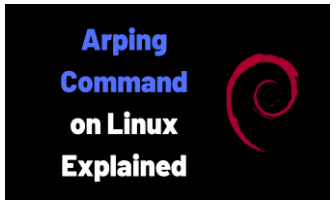
Tools/Assess Organizational Security

Network Reconnaissance and Discovery

ping/pathping

netstat

netcat



arp

Tools/Assess Organizational Security

Network Reconnaissance and Discovery

route

curl

theHarvester

scanless

Tools/Assess Organizational Security

Network Reconnaissance and Discovery

dnsrecon

Nessus

Cuckoo

File Manipulation

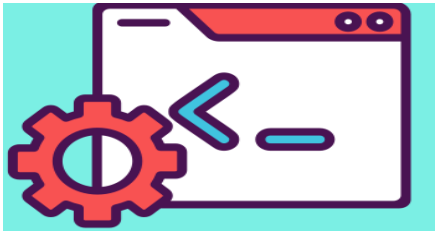
head

tail

cat

grep

chmod



logger

Shell and Script Environments

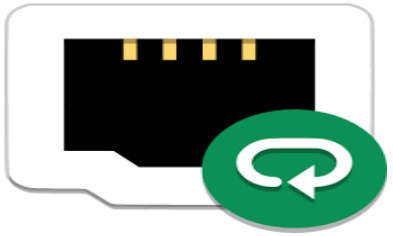
SSH

PowerShell

python

openssl

Packet Capture and Replay



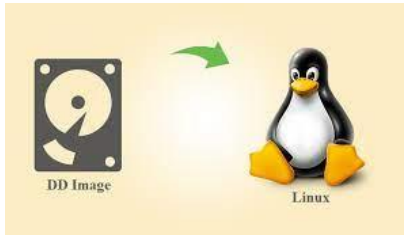
Tcpreplay

tcpdump

Wireshark

Tools/Assess Organizational Security

Forensics tools



dd

memdump

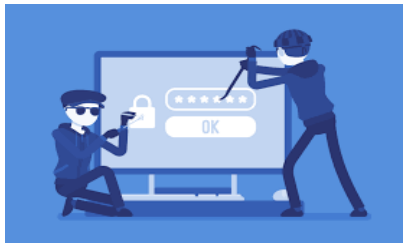
WinHex

FTK Imager

Autopsy

Tools/Assess Organizational Security

Exploitation Frameworks



Password Crackers

Metasploit

Core impact

Incident Response Policies, Processes, and Procedures

Incident Response Policies, Processes, and Procedures

This chapter covers CompTIA Security+ exam objective 4.2: Summarize the importance of policies, processes, and procedures for incident response.

Incident response is the methodology an organization uses to respond to and manage a cyberattack.

Incident Response Plans

An incident response plan describes the steps an organization performs in response to any situation determined to be abnormal in the operation of a computer system or network. The causes of incidents are many—from the environment (storms), to user error, to unauthorized actions by unauthorized users, to name a few.

Incident Response Policies, Processes, and Procedures

Incident Response Process

The incident response process is the set of actions security personnel perform in response to a wide range of triggering events. These actions are broad and varied, as they have to deal with numerous causes and consequences. Incident response activities at times are closely related to other IT activities involving IT operations.

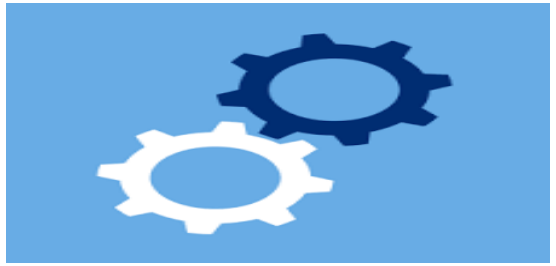
Incident Response Policies, Processes, and Procedures

Incident Response Phases

Preparation

Identification

Containment



Eradication

Recovery

Lessons Learned

Incident Response Policies, Processes, and Procedures

Preparation phase

- Ensure your team are properly trained regarding their incident response roles and responsibilities in the event of data breach
- Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.
- Ensure that all aspects of your incident response plan (training, execution, hardware and software resources, etc.) are approved and funded in advance

Questions to address

- Has everyone been trained on security policies?
- Have your security policies and incident response plan been approved by appropriate management?
- Does the Incident Response Team know their roles and the required notifications to make?
- Have all Incident Response Team members participated in mock drills?

Identification phase

In this phase you will determine whether you've been breached.
A breach, or incident, could originate from many different areas.

Questions to address

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?

Incident Response Policies, Processes, and Procedures

Containment phase

- What's been done to contain the breach short term?
- What's been done to contain the breach long term?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of backups are in place?
- Does your remote access require true multi-factor authentication?
- Have all access credentials been reviewed for legitimacy, hardened and changed?
- Have you applied all recent security patches and updates

Incident Response Policies, Processes, and Procedures

Eradication phase

In this phase you need to be thorough. If any trace of malware or security issues remain in your systems, you may still be losing valuable data, and your liability could increase.

Questions to address

Have artifacts/malware from the attacker been securely removed?
Has the system be hardened, patched, and updates applied?
Can the system be re-imaged?

Incident Response Policies, Processes, and Procedures

Recovery Phase

During this time, it's important to get your systems and business operations up and running again without the fear of another breach..

Questions to address

When can systems be returned to production?
Have systems been patched, hardened and tested?
Can the system be restored from a trusted back-up?
How long will the affected systems be monitored and what will you look for when monitoring?
What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc.)

Incident Response Policies, Processes, and Procedures

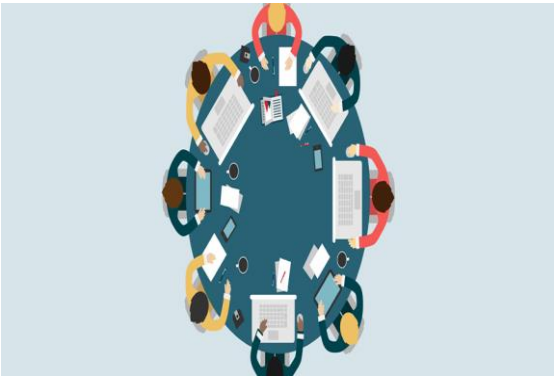
Lesson learned

Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the data breach.

Questions to address

What changes need to be made to the security?
How should employee be trained differently?
What weakness did the breach exploit?
How will you ensure a similar breach doesn't happen again?

Cyber Security Exercises



Tabletop

Walkthroughs

Simulations

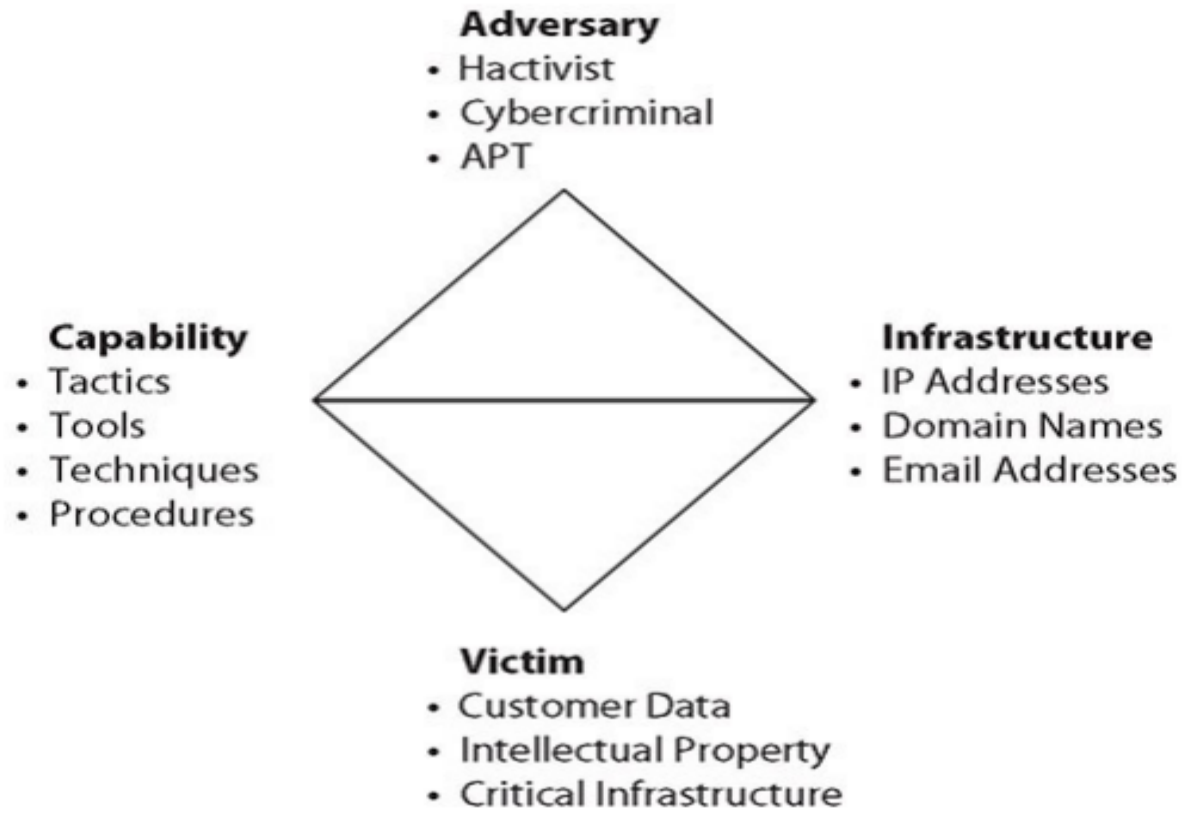
Attack Frameworks

Attack frameworks provide a roadmap of the types of actions and sequence of actions used when attacking a system. Frameworks bring a sense of structure and order to the multidimensional problem associated with defending a variety of systems against multiple different types of attackers with various objectives.

The MITRE ATT&CK framework is a comprehensive matrix of attack elements, including the tactics and techniques used by attackers on a system. This framework can be used by threat hunters, red teamers, and defenders to better classify attacks and understand the sequential steps an adversary will be taking when attacking a system.

The Diamond Model of Intrusion Analysis

The Diamond Model of Intrusion Analysis is a cognitive model used by the threat intelligence community to describe a specific event. It is based on the notion that an event has four characteristics



Cyber Kill Chain

The Cyber Kill Chain is a model developed by Lockheed Martin as a military form of engagement framework. This model has a series of distinct steps that an attacker uses during a cyberattack—from the early reconnaissance stages to the exfiltration of data.

Incident Response Policies, Processes, and Procedures

Stakeholder Management

Communication Plan

Disaster Recovery Plan

Business Continuity Plan

Continuity of Operation Planning (COOP)

Incident Response Team

Digital Forensics

Digital Forensics

This chapter covers CompTIA Security+ exam objective 4.3: Explain the key aspects of digital forensics.

Documentation/Evidence

Direct evidence Oral testimony that proves a specific fact (such as an eyewitness's statement). The knowledge of the facts is obtained through the five senses of the witness, with no inferences or presumptions.

Real evidence Also known as associative or physical evidence, this includes tangible objects that prove or disprove a fact. Physical evidence links the suspect to the scene of a crime

Documentary evidence Evidence in the form of business records, printouts, manuals, and the like. Much of the evidence relating to computer crimes is documentary evidence.

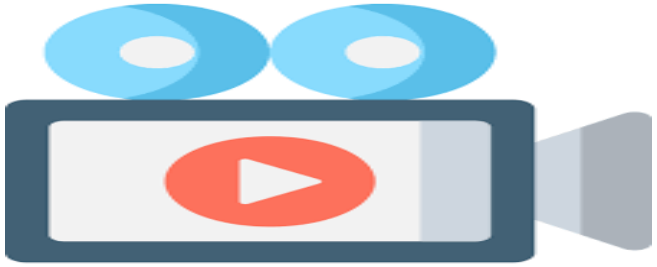
Digital Forensics

Legal Hold

In the U.S. legal system, legal precedent requires that potentially relevant information be preserved at the instant a party "reasonably anticipates" litigation or another type of formal dispute.

Video

A convenient method of capturing significant information at the time of collection is video capture



Digital Forensics

Admissibility

For evidence to be credible, especially if it will be used in court proceedings or in corporate disciplinary actions that could be challenged legally, it must meet three standards

• Sufficient evidence The evidence must be convincing or measure up without question.
• Competent evidence The evidence must be legally qualified and reliable.
• Relevant evidence The evidence must be material to the case or have a bearing on the matter at hand.

Digital Forensics

- **Best evidence rule** Courts prefer original evidence rather than a copy, to ensure that no alteration of the evidence (whether intentional or unintentional) has occurred.
- **Exclusionary rule** The Fourth Amendment to the U.S. Constitution precludes unreasonable search and seizure. Therefore, any evidence collected in violation of the Fourth Amendment is not admissible as evidence.
- **Hearsay rule** Hearsay is secondhand evidence—evidence offered by the witness that is not based on the personal knowledge of the witness but is being offered to prove the truth of the matter asserted.

EVIDENCE

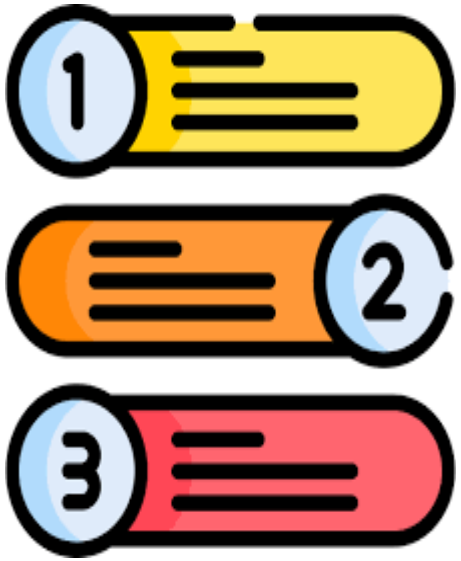
Chain of Custody

After evidence is collected, it must be properly controlled to prevent tampering. The chain of custody accounts for all persons who handled or had access to the evidence. More specifically, the chain of custody shows who obtained the evidence, when and where it was obtained, where it was stored, and who had control or possession of the evidence for the entire time since the evidence was obtained. Any and all access to the evidence is recorded.

Chain of Custody

The following are the critical steps in a chain of custody:

1. Record each item collected as evidence.
2. Record who collected the evidence along with the date and time it was collected or recorded.
3. Write a description of the evidence in the documentation.
4. Put the evidence in containers and tag the containers with the case number, the name of the person who collected it, and the date and time it was collected or put in the container.
5. Record all message digest (hash) values in the documentation.
6. Securely transport the evidence to a protected storage facility.
7. Obtain a signature from the person who accepts the evidence at this storage facility.
8. Provide controls to prevent access to and compromise of the evidence while it is being stored



Digital Forensics

Timelines of Sequence of Events

Timestamps

Time offset

Tags

Reports